Field Theory and Galois Theory

A Project Report

submitted by

Amit Kumar

in partial fulfilment of the requirements
for the award of the degree
of

MASTER OF SCIENCE
IN MATHEMATICS

2011

DEPARTMENT OF MATHEMATICS
NATIONAL INSTITUTE OF TECHNOLOGY ROURKELA
ROURKELA, ORISSA-769008

THESIS CERTIFICATE

This is to certify that the Project Report entitled **"Field Theory and Galois Theory"** submitted by *Amit Kumar* to National Institute of Technology Rourkela, Orissa for the partial fulfilment of the requirements of M.Sc. degree in Mathematics is a bonafide record of review work carried out by him under my supervision and guidance. The content of this project, in full or in parts, has not been submitted to any other Institute or University for the award of any degree or diploma.

(S.R.Pattanaik)

and

(R.S.Tungala)

Asst.Professor

Department of Mathematics

NIT Rourkela

DECLARATION

I declare that the topic '*Field Theory and Galois Theory*' for my M.Sc. degree has not been submitted in any other institution or university for the award of any other degree or diploma.

Place: Amit Kumar

Date: Roll.No. 409MA2068

ACKNOWLEDGEMENT

I would like to warmly acknowledge and express my deep sense of gratitude and indebtedness to my guides **Dr S.R.Pattanaik and Dr. R.S.Tungala**,
Asst Professor, Department of Mathematics, NIT Rourkela, Orissa, for his keen guidance, constant encouragement and prudent suggestions during the course of my study and preparation of the final manuscript of this Project.

I would like to thank the faculty members of Department of Mathematics for allowing me to work for this Project in the computer laboratory and for their cooperation.

My heartfelt thanks to all my friends for their invaluable co-operation and constant inspiration during my Project work.

I owe a special debt gratitude to my revered parents, my brother, sister for their blessings and inspirations.

Rourkela,769008
May,2011

(Amit Kumar)
M.Sc. Mathematics
NIT Rourkela

No	Contain	page no

Introduction

The general solutions of linear and quadratic polynomial in one variable were known centuries before. For cubic and quartic equations also the general solutions are provided by Cardano's and Ferrari's methods respectively. In 19^{th} century a great work has been done to find general solution of a general polynomial by radicals. However there was no success even after efforts of many great mathematicians of that time. Eventually work by Able and Galois gives satisfactory solution and complete understanding of this problem.

Galois Theory provides a connection between Field theory and Group theory, which in turn useful to convert problems in field theory into Group theory, which are better understood and easy to handle. Galois theory not only provide answer to the problem discussed above but also explains why the general solution exists for polynomials with degree less then or equal to 4.

In his original work, Galois used permutation groups to describe relations between roots of the polynomial. In modern approach, developed by Artin, Dedekind etc., involves study of automorphisms of field extensions.

CHAPTER- 1

Euclidean Domain, Principal Ideal Domains and Unique Factorization Domains. Polynomial Rings & Irreducibility Criteria.

Motivation:-

There are a number of classes of rings with more algebraic structure than generic rings. Those considered in this chapter are rings with a division algorithm (Euclidean Domains), rings in which every ideal is principal (Principal ideal Domains) and rings in which element have factorization into primes (Unique Factorization Domains). The principal examples of such rings are the ring Z of integers and polynomial rings F[x] with coefficients in some field F.

[2]EUCLIDEAN DOMAINS

In Z , the absolute value or $|n| \in Z$, is non-negative number. Given $a, b \in Z$, $b \neq 0$ such that

$$a = bq + r, \text{ where } 0 \leq |r| < |b|$$

Definition:- An integer domain R is called Euclidean Domain if $\exists$ a function

$\Phi : R \mid \{0\} \longrightarrow Z \geq 0$ satisfying

[non-zero element of R to the non-negative integers, Φ is norm]

1. $\Phi(a) \leq \Phi(b)$ for all element a, b in R
2. Given $a, b \in R$, $b \neq 0$ $\exists$ $q, r \in R$ such that $a = bq + r$ and either $r=0$ or $\Phi(r) \leq \Phi(b)$.

Examples :-

1. The ring Z is Euclidean domain with $\Phi(n)=|n|$

Ans :-

i . Let $m,n \in Z$ $\Phi(n)=|n|$ $\Phi(m)=|m|$

Then $\Phi(nm)=|nm|$

Now we have

$\Phi(n)=|n| \leq |n||m|= \Phi(nm)$

$\Phi(n) \leq \Phi(nm)$.

ii. $m, n \in Z$, $n \neq 0$ $\exists$ q , r such that $m= n q + r$ and $|r| < |n|$.

(2) Let F be a field ,then F[x] for $f[x] \neq 0 \in F[x]$

Define $\Phi(f) = \deg f$

Ans:-

i. Let $f, g \in F[x]$ such that

$\Phi(f) = \deg f$

$\Phi(f) = \deg g$

$\Phi(fg) = \deg(fg)$

$\Phi(f) = \deg f \leq \deg(fg) = \Phi(fg)$

ii. 2^{nd} condition is follows from the division algorithm for F[x].

Principle Ideal Domain:-

An integer domain R is called P.I.D if every ideal of R is principal. [Principal Ideal: - Ideal generated by one element]

i.e. every ideal has the form $< a > = \{ ra \mid r \in R\}$ for some $a \in R$

Example :-

i. The ring Z is a P.I.D generated by $< n >$

ii. A field F is P.I.D. The only ideal of F are {0} and F itself.

iii. Let F be a field, then F[x] is a P.I.D

Ans:-

We know that F[x] is integral domain.

Let us consider I be an ideal in F[x]

If $I = \{0\}$ then $I = < 0>$

If $I \neq \{0\}$ then among all the elements of I,

Again let g(x) be one of the minimum degree.

Claim: I = < g(x) >

As g(x) ∈ I

We have < g(x) > ⊆ I

Only to show I ⊆ < g(x) >

Let f(x) ∈I, then by division algorithm, we can write

f(x) = g(x) q(x) + r(x)

Where r(x) = 0 or deg r(x) < deg g(x)

$\Longrightarrow$ r(x) = f(x) – g(x)q(x) ∈ I [As f(x), g(x)∈I]

so, r(x) = 0 [As deg r(x) < deg g(x) which is not possible as the minimality of deg g(x)]

$\Longrightarrow$f(x) = g(x) q(x)

$\Longrightarrow$f(x) ∈ < g(x) >

$\Longrightarrow$I ⊆ < g(x) >

iv. The ring Z[x] is an integral domain but not P.I.D

Solution:

Let us consider the ideal ‘S’ of Z[x] generated by the elements 2 and x of Z[x], then

S = 2 f(x) + xg(x) ; f(x), g(x) ∈ Z [x]

Assume Z[x] is P.I.D and generated by < h(x) >

Say h(x) ∈ Z(x)

i.e. Z(x) = { < h(x) > : h(x) ∈ Z[x] }

2 ∈ S $\Longrightarrow$2 ∈ < h(x)>

$\Longrightarrow 2 = h(x)\, h_1(x)$ for some $h_1(x) \in Z[x]$

$x \in S \Longrightarrow x \in < h(x) >$

$\Longrightarrow x = h(x)\, h_2(x)$ for some $h_2(x) \in Z[x]$

Therefore $2h_2(x) = xh_1(x)$

$\Longrightarrow$ Each co-efficient of $h_1(x)$ is an even-integer. So $h_1(x) = 2\, p(x)$ for some $p(x) \in Z[x]$

So, $2 = 2h(x)\, p(x)$

$\Longrightarrow h(x)\, p(x) = 1$

$\Longrightarrow 1 \in < h(x) >$ i.e. $1 \in S$

Now $1 \in S$

$\Longrightarrow 1 = 2q(x) + xr(x)$ for some $q(x),\ r(x) \in Z[x]$

Let $q(x) = a_0 + a_1 x + a_2 x^2 + \ldots$

$r(x) = b_0 + b_1 x + b_2 x^2 + \ldots$

Then $1 = 2(a_0 + a_1 x + a_2 x^2 + \ldots) + x(b_0 + b_1 x + b_2 x^2 + \ldots)$

$\Longrightarrow 1 = 2a_0$

Which is not possible as a_0 is an integer. Contradicts the assumption, so Z [x] is not a P.I.D.

Unique Factorization Domain :-

An integer domain R is called an U.F.D if every non-zero elements of $r \in R$ which is not an unit has the following two properties**:-**

i) r can be written as the products of irreducible in R (not necessary distinct)

i.e. $r = p_1, p_2, \ldots p_n$ and

ii) The decomposition of ---- (1) is unique up to associates**.**

i.e. if $r = q_1, q_2, \ldots q_m$ is another factorization of r into irreducible then m= n and there is some renumbering of the factors so that p_i is associates to q_i for i=1, 2**, . . . ,** n

Example:- (i) The integral domain Z is U.F.D **.** Every non-zero elements other than 1 and **-**1 in Z can be expressed as the product of a finite number of irreducible elements in Z and the factorization is unique except for the order of the factors**.**

12= 2·2 · 3 = (-2) · 2 · (-3) = (-2)**.**(-3) ·2

These factorization are some except for the order and the associates of the irreducible.

(ii) Z is U.F.D so integral domain Z[x] is a U.F.D**.**

(iii) The domain D= Z[$\sqrt{-5}$] is not a U.F.D

Solution:

6 has two different factorization into irreducible as $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$

In D, each $2 \cdot 3$, $1 + \sqrt{-5}$, $1 - \sqrt{-5}$ is irreducible in D .

$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$

None of the factors $(1 + \sqrt{-5})$ and $(1 - \sqrt{-5})$ associates of 2 or 3 . Since 1 and -1 are only units in D.

[2]Conclusion: - Finally as above our discussion we find the relation as

Fields $\Longrightarrow$ E.D $\Longrightarrow$ P.I.D $\Longrightarrow$ U.F.D $\Longrightarrow$ I.D

But in each of cases converse part is not true. Which are shown by the examples:-

i. Z is E.D but not field

ii. $Z[\frac{1 + \sqrt{-19}}{2}]$ is P.I.D but not E.D

iii. Z [x] is U.F.D but not P.I.D

iv. $Z[\sqrt{-5}]$ is I.D but not U.F.D

[1]Polynomial rings and irreducible criteria

Let R be a commulative Ring. The set of formal symbols.

$R[x]=\{ a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \mid a_i \in R, n \text{ is an nonnegative integer } \}$

is called the ring of polynomials over R in the indeterminant x.

If $a_n \neq 0$ then the polynomial degree 'n' and $a_n x^n$ is the leading term .

The polynomial is monic if $a_n = 1$.

Content of polynomial, primitive polynomials:

The content of a nonzero polynomial $a_n x^n + a_n x^n + \ldots + a_1 x + a_0$, where a's are integers, is the greatest common divisor of the integers a_n , a_{n-1} , . . . ,a_0 . A primitive polynomial is element of Z[x] with content 1.

Irreducible polynomial, reducible polynomial

A non-constant polynomial f(x) is irreducible over F[x], if f(x) cannot be expressed as a product of g(x) h(x) of two polynomials g(x) and h(x) in F[x] both of lower degree than the degree of f(x).

If f(x) ∈F[x] is a non-constant polynomial that is not irreducible over F then f(x) is reducible over F.

Theorem: let f(x) ∈ F[x]and let f(x) be of degree 2 or 3 then f(x) is reducible over F if and only if it has a zero in F.

Proof:

Let f(x) is reducible over F

To show : f(x) has a zero in F

As f(x) is reducible so we can write

f(x) = g(x) h(x), where degree of g x) and h(x)are both less than the degree of f(x), then since f(x) is either quadratic or cubic, either g(x) or h(x) is of degree 1.

If say g(x) is of degree 1 , then expect for a possible factor in F , g(x) is the form x-a

Then g(a) = 0

$\Longrightarrow$ f(a) = 0

So, f(x) has a zero in F

Conversely from the factor theorem we know that , if f(a) = 0 for a $\in$ F , then x-a is a factor of f(x).

So f(x) is reducible.

Example : i) X^2 - 2 $\in$ Q[x] has no zero in Q . This shows that x^2- 2 is irreducible over Q.

ii) In particular it is easy to use when the field is Z_p .

As in Z_2 polynomial $x^2 + x + 1$ is irreducible. As it has no root .

i.e. f (0) = 0 + 0 + 1 = 1

and f(1) = 1 + 1 + 1 = 3 = 1

[1]Gauss's Lemma:

Statement → The product of two primitive polynomials is primitive.

Proof :

let f(x) and g (x)be primitive polynomials .To prove f (x) g(x) is primitive

If possible, let f(x)g(x) is not primitive

So let p be a primitive divisor of the content of f(x)g(x)

And let the polynomials f'(x) and g'(x) and (f (x) g(x))' obtained from f(x), g(x) and f(x)g(x) respectively, by reducing the co-efficients modulo p. Then f'(x) and g'(x) belongs to integral domain Z_p[x]and

f'(x) g'(x) = (f (x) g(x))' = 0, the zero elements of Z_p[x]

So, either f'(x) = 0 or g'(x) = 0

[Since these are in integral domain]

This means that either p divides every coefficient of f(x) or p divides every coefficient of g(x).

Therefore either f(x) is not primitive or g(x) in not primitive, which is contradiction the assumption.

So f(x) g(x) is primitive .Hence the statement.

[1] Over Q implies over Z

Let $f(x) \in Z[x]$. If $f(x)$ is reducible over Q, then it is reducible over Z

Proof:

Given $f(x)$ is reducible over Q, so we can write $f(x) = g(x)\, h(x)$, where $g(x)$ and $h(x) \in Q(x)$ we may assume that $f(x)$ is primitive because we can divide both $f(x)$ and $g(x)\, h(x)$ by the content of $f(x)$.

Let a be the l.c.m of the denominators of the coefficients of g(x) and b be the l.c.m of the denominators of the coefficient of $h(x)$.

Then $abf(x) = ag(x) . bh(x)$, where $ag(x)$ and $bh(x) \in Z[x]$

Let c_1 be the content of $ag(x)$ and

c_2 be the content of $bh(x)$

Then $ag(x) = c_1 g_1(x)$ and

$bh(x) = c_2 h_1(x)$

Where $g_1(x)$ and $h_1(x)$ both are primitive

and $ab\, f(x) = c_1 c_2 g_1(x) h_1(x)$ …….(1)

$f(x)$ is primitive so content of $abf(x)$ is ab and $g_1(x)\, h_1(x)$ is primitive [$\because$ product of two primitive polynomials is primitive]

So content of $c_1 c_2 g_1(x) h_1(x)$ is $c_1 c_2$

Thus from ……..(i)

$ab = c_1 c_2$

$f(x) = g_1(x)\, h_1(x)$

Where $g_1(x)$ and $h_1(x) \in Z[x]$ and

deg $g_1(x)$ = deg $g(x)$ and deg $h_1(x)$ = deg $h(x)$

IRREDUCIBILITY TESTS:

1) Mod p irreducibility test

Statement: let p be a prime and suppose that $f(x) \in Z[x]$ with $\deg f(x) \geq 1$. Let $f'(x)$ be the polynomial in $Z_p[x]$ obtained from $f(x)$ modulo p. If $f'(x)$ is irreducible over Z_p and $\deg f'(x) = \deg f(x)$, then $f(x)$ is irreducible over Q.

Proof:

Let $f(x) \in Z[x]$

If possible let $f(x)$ is reducible over Q then we have

$f(x) = g(x)\, h(x)$ with $g(x), h(x) \in Z[x]$

and both $g(x)$ and $h(x)$ have degree less than that of $f(x)$

let $f'(x)$, $g'(x)$ and $h'(x)$ be the polynomials obtain from $f(x)$, $g(x)$ and $h(x)$ by reducing all the co-efficient modulo p .

Since $\deg f(x) = \deg f'(x)$

we have $\deg g'(x) \leq \deg g(x) < \deg f'(x)$

again $\deg h'(x) \leq \deg h(x) < \deg f'(x)$

but $f'(x) = g'(x)\, h'(x)$

$\Rightarrow$ $f'(x)$ is reducible over Z_p ,

which is contradiction

Hence $f(x)$ is irreducible over Q.

Example: $f(x) = 11x^4 + 8x^3 + 5x^2 + 5$. Then over Z_2 , we have

$f'(x) = x^4 + x^2 + 1$ and

since $\deg f(x) = \deg f'(x)$

$f'(0) = 1$ and $f'(1) = 1 + 1 + 1 = 3 = 1$

we find that $f'(x)$ is irreducible over Z_2

Thus $f(x)$ is irreducible over Q.

2) Eisenstein's Criterion:-

In 1980 Ferdin and Eisenstein, a student of Gauss, was found another important irreducibility test . [1]

Statement :-

let

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in Z[x]$

If there is a prime p such that $p \nmid a_n$,$p \mid a_{n-1}, \ldots, p \mid a_o$ and $p^2 \nmid a_0$ then f(x) is irreducible over Q

Proof :-

If possible let f(x) is reducible over Q.

Then we know that ∃ elements g(x) and h(x) in Z[x] such that

f(x)=g(x)h(x) and

deg g(x) ≥ 1 ,deg h(x) < n

Say $g(x)= b_r x^r + \ldots + b_0$ and

$h(x)= c_s x^s + \ldots + c_0$

Then since $p \mid a_0$, $p^2 \nmid a_0$

and $a_0=b_0c_0$,

It follows that p divides one of b_0 and c_0 but not the other

Let us consider the case $p \mid a_0$but $p \nmid c_0$

$\because p \nmid a_n \Rightarrow p \nmid b_r c_s$

$\Longrightarrow p \nmid b_r$ or $p \nmid c_s$

$p \nmid b_r$ so there is a least ineger 't' such that $p \nmid b_t$

Now consider

$a_t = b_t c_o + b_{t-1} c_1 + \ldots + b_0 c_t$.

By assumption, p divides a_t and by choice of t every summand on the right hand side after the first one is divisible by p .

Then it is true that p to divides $b_t c_0$, this is impossible .

$\because$ p is prime and p divides neither b_t nor c_0 which gives contradiction

Hence the statement .

Example :-

Taking p = 5 , $f(x) = 18\,x^5 - 5x^4 - 10x^2 - 102$ is irreducible over Q by Eisenstein's criterion,

because $5 \nmid 18$ and $25 \nmid 102$ but 5 does divide -5 and -10.

Important Corollary :-

Let F be a field and p(x) an irreducible polynomial over F.

Then $F[x] \mid < p(x) >$ is a field .

CHAPTER-2

Fields Theory-Extension Fields, Algebraic Extentions.

Characteristic of field:-

Is denoted by char (F) and defined as smallest positive integer P such that

$P.1_F = 0$, where 1_F is the identity of F

- Characteristic of a field is either '0' or a prime 'P'.

Extension Field: - A Field E is an extension field of a field F if $F \subseteq E$ and the operation of F are those of E restricted to F. Denoted by E|F

Ex: - C

R

Q

E (Extension Field)

F (Base Field)

FUNDAMENTAL THEOREM OF FIELD THEORY (KRONECKER'S THEOREM, 1887) [1]

Let F be a field and f(x) a non-constant polynomial in F[x]. Then there is an extension field E of F in which f(x) has a zero.

Proof: - As F[x] is a U.F.D., hence by definition of U.F.D f(x) has an irreducible factor, say it p(x).

Now, it is sufficient to construct an extension field E of F in which p(x) has a zero.

Hence, E= F[x]|<p(x)>

Also, since the mapping $\varphi : F \longrightarrow E$, given by $\varphi(a) = a + \langle p(x) \rangle$ is one-one and preserves both operations.

E has a subfield isomorphic to F.

Enough to show that p(x) has zero in E.

Let $p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$

Then, in E, $\bar{x} = x + \langle p(x) \rangle$ is a zero of p(x).

$p(x+\langle p(x)\rangle) = a_n (x+\langle p(x)\rangle)^n + a_{n-1} (x+\langle p(x)\rangle)^{n-1} + \ldots + a_0$

$= a_n (x^n + \langle p(x)\rangle) + a_{n-1} (x^{n-1} + \langle p(x)\rangle) + \ldots + a_0$

$= a_n x^n + a_{n-1} x^{n-1} + \ldots\ldots\ldots + a_0 + \langle p(x)\rangle$

$= P(x) + \langle p(x)\rangle$

$= 0 + \langle p(x)\rangle$

$= \langle p(x)\rangle$

Example:-

Let F=R and let $f(x) = x^2 + 1$ clearly $x^2 + 1$ is irreducible over R. Then $\langle x^2 + 1\rangle$ is a maximal ideal in R[x], so $R[x]/\langle x^2 + 1\rangle$ is a field. Let $r \in R$ with $r + \langle x^2 + 1\rangle$ in $R[x] / \langle x^2 + 1\rangle$,

Here, R is a subfield of $E = R[x]/\langle x^2 + 1\rangle$

Let $\alpha = x + \langle x^2 + 1\rangle$

Now,

$\alpha^2 + 1 = (x+\langle x^2 + 1\rangle)^2 + 1$

$= (x^2 + 1) + \langle x^2 + 1\rangle$

$= 0$

Thus α is a zero of $x^2 + 1$

SPLITTING FIELDS:-

The extension field E of F is called splitting field for the polynomial $f(x) \in F[x]$, if $f(x)$ factors completely into linear factor in $E[x]$ and $f(x)$ does not factor completely into linear factor over any proper subfield of E containing F.

Examples:-

(i) The splitting field for $x^2 - 2$ over Q is just $Q(\sqrt{2})$ as $x = \pm\sqrt{2}$ and $-\sqrt{2} \in Q(\sqrt{2})$

(ii) The splitting field of $(x^2 - 2)(x^2 - 3)$ is field $Q(\sqrt{2}, \sqrt{3})$

(iii) Let $f(x) = x^2 + 1 \in Q[x]$

$x^2 + 1 = (x + \sqrt{-1})(x - \sqrt{-1})$, here $f(x)$ splits in ℂ, but a splitting over Q is

$Q(i) = \{r + si / r, s \in Q\}$

But $x^2 + 1 \in R[x]$, here splitting field for $(x^2 + 1)$ over R is ℂ.

Existence of splitting fields

Let F be a field and let $f(x)$ be a non-constant element of $F[x]$. Then there exists a splitting field E for $f(x)$ over F.

Proof:-

We prove it by induction on deg $f(x)$.

If deg $f(x) = 1$, then $f(x)$ is already linear and $E = F$.

Now suppose that the statement is true for all fields and all polynomial of degree less than that of $f(x)$.

Hence by Fundamental Theorem of Field Theory, there is an extension E of F in which $f(x)$ has a zero, say a_1

$f(x) = (x - a_1)\, g(x)$, where $g(x) \in E[x]$.

since deg g(x) < deg f(x), by induction, there is a field M that contains E and all the zeros of g(x), say, a_2 , a_3 , . . . a_n . Clearly, then, a splitting field for f(x) over F is F (a_1 , a_2, . . . , a_n)

Splitting Fields are unique:-

Let Φ be an isomorphism from a field F to a field F' and let f(x) ∈ F[x]. If E is a splitting field for f(x) over F and E' is a splitting field for Φ (f(x)) over F, then there is an isomorphism from E to E' that agrees with Φ on F [i.e. splitting fields are unique] .

Proof: We prove it by induction on deg f(x). If deg f (x) =1, then E=F and E' = F'. So that Φ is itself the required mapping. If deg f(x)>1, let p(x) be an irreducible factor of f(x), let a be a zero of p(x) in E, and let b be a zero of Φ (p(x)) in E'. By known lemma, there is an isomorphism α from F (a) to F' (b) that agrees with Φ on F and carries a to b.

Now, f(x) = (x-a) g(x), where g(x) ∈ F (a)[x]

Then E be a splitting field of g(x) over F (a)

E' be a splitting field of α (g(x)) over F'(b)

Since deg g(x) < deg f(x), there is an isomorphism from E to E' that agrees with α on F(a) and therefore with Φ on F.

Theorem:-

Let F be a field and let p(x) ∈ F[x] be irreducible over F. If a is a zero of p(x) in some extension E of F, then F (a) is isomorphic to F[x] / <p(x)>. Furthermore, if deg p(x) =n, then every member of F (a) can be uniquely expressed in the form

$C_{n-1}\, a^{n-1} + C_{n-2}\, a^{n-2} + \ldots + c_1 a + c_0$,

Where c_0, c_1 , . . . $c_{n-1} \in$ F.

Examples:-

In a language of vector space,if ‘a’ is a zero of an irreducible polynomial over F of degree n, then the set $\{1,a,a^2,\ldots,a^{n-1}\}$ is a basis for F (a) over F. Consider the irreducible polynomial $f(x) = x^6-2$ over Q. Since $\sqrt[6]{2}$ is a zero of f(x), so as above theorem, we have the set $\{1, 2^{1/6}, 2^{2/6}, 2^{3/6}, 2^{4/6}, 2^{5/6}\}$ is a basis for $Q(\sqrt[6]{2})$ over Q.

Thus,

$$Q(\sqrt[6]{2}) = \{a_0 + a_1 + 2^{1/6} + a_2\, 2^{2/6} + a_3\, 2^{3/6} + a_4\, 2^{4/6} + a_5\, 2^{5/6} \mid a_i \in Q\}$$

This Field is isomorphic to $Q[x] |< x^6-2>$.

[1]Algebraic Extensions

Let F be a field and let E be an extension of F. An elements $\alpha \in E$ is said to be algebraic over F if α is a root of some non-zero polynomial $f(x) \in F[x]$. [I.e. $f(\alpha) = 0$].

If α is not algebraic over F, then ‘α’ is said to be transcendental over F.

An extension E of F is called algebraic extension of F if every elements of E is algebraic over F. If E is not an algebraic extension of F, then it is called a transcendental extension of F.

e.g.: e is transcendental over Q,

π is transcendental over Q.

But it is not known about (π+e)

[3]Characteristics of Extension:

Let E be an extension field of a field F and let a ϵ E be algebraic over F. Let p(x) ∈F[x] be a polynomial of least degree such that p(a) =0. Then

I. P(x) is irreducible over F.

II. If g(x) ∈ F[x] is such that g (a) =0, then p(x)| g(x).

III. There is exactly one monic polynomial p(x) ∈ F[x] of least degree such that p(a)=0

Proof:

(i) Let p(x) is reducible over F. $p(x) = p_1(x)\, p_2(x)$ and degree of $p_1(x)$, degree of $p_2(x)$ be less than that of p(x).

Then $0=p(a) = p_1(a).\, p_2(a)$

=> Either $p_1(a) = 0$ [As field]

or $p_2(a)=0$

i.e. 'a' satisfy a polynomial of degree less than p(x), a contradiction

So p(x) is irreducible over F.

(ii) Since g(x) ∈ F[x],

By division algorithm

$g(x) = p(x)\, q(x) + r(x)$, where r(x)=0 or deg r(x)< deg p(x)

Then,

$g(a) = p(a).\, q(a) + r(a)$

i.e. r(a)=0

As p(x) is least degree among the polynomial satisfying by a,

i.e. r(x) =0

Thus p(x) |g(x)

(iii) Let g(x) be a monic polynomial of least degree such that g(a)=0

Then by (ii) p(x)| g(x) and g(x) |p(x)

$\Longrightarrow$ p(x) = g(x) (since both are monic)

Degree of Extension:

Let E be a field extension of a field F, we may view that E is vector space over F. The degree of field extension E|F is denoted by [E: F] and defined as-

deg [E: F] = dimension of E over F

If [E: F] =n

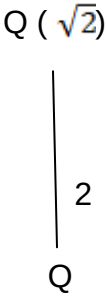
E has a degree n over F.

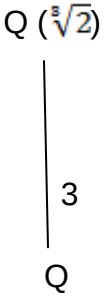
If E has dimension n as a vector space over F.

If [E: F] is finite, E is called a finite extension of F; otherwise, we say that E is an infinite extension of F.

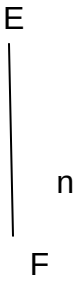
Example:

1. The field of complex numbers has degree 2 over the reals since {1, i} is a basis.
2. If a is algebraic over F and its minimal polynomial over F has degree n, then we have {1, a . . . a^{n-1}} is a basis for F (a) over F; and therefore [F(a):F]=n. In this case, we say that a has degree n over F.





[Q ($\sqrt{2}$): Q] =2 [Q($\sqrt[3]{2}$) :Q] =3 [Q($\sqrt[6]{2}$) :Q] =6



[E: F]= n

Theorem:-

Finite Implies Algebraic

If E is a finite extension of F, then E is algebraic extension of F.

Proof: Suppose that [E: F] = n and a ϵ E. Then the set {1, a, . . . ,a^n} is linearly dependent over F; so there are elements c_0, c_1, . . . , c_n in F, not all zero, such that $c_n a^n + c_{n-1} a^{n-1} + c_{n-2} a^{n-2} +. . . + c_1a+c_0 = 0$

So 'a' satisfy $c_n a^n + c_{n-1} a^{n-1} + c_{n-2} a^{n-2} +. . . .+ c_1a+c_0 = 0$

so 'a' is algebraic over F.

(*) But the converse of the above theorem is not true which is shown in the following example

e.g. $Q\ (2^{1/2}, 2^{1/3}, 2^{1/4}, \ldots, 2^{1/n}, \ldots)$

Q

Let $X = 2^{1/n}$

$\Rightarrow X^n - 2 = 0$

So algebraic extension as $(a^n - 2 = 0)$

Clearly it is not finite extension.

Theorem:-

$[K: F] = [K: E]\,[E: F]$

Let K be a finite extension field of the field E and let E be a finite extension field of the field F. Then K is finite extension of the field F and $[K: F] = [K: E]\,[E:F]$

Proof: Let $X = \{ x_1, x_2, \ldots, x_n \}$ be a basis for K over E and

Let $Y = \{y_1, y_2, \ldots, y_n\}$ be a basis for E over F.

It remains to prove that

$YX = \{y_i x_i \mid 1 \le j \le m, 1 \le i \le n\}$ is a basis for K over F.

For this, let $a \in k$

Then there are elements $b_1, b_2, \ldots, b_n \in E$ such that

$a = b_1x_1 + b_2x_2 + \ldots + b_nx_n$

and, for each i= 1,. . . , n, there are elements $c_{i1}, c_{i2}, \ldots, c_{im} \in F$ such that

$b_i = c_{i1}y_1 + c_{i2}y_2 + \ldots + c_{im}y_m$

Thus,

$a = \sum_{i=1}^{n} bi\ xi = \Sigma^{n}_{i=1}\ (\sum_{j=1}^{m} c_{ij}y_j)x_i$

$= \sum_{i,j} c_{ij}(y_j x_i)$

This proves that YX spans K over F. Now suppose there are elements c_{ij} in F such that $0= \Sigma_{i,j}\ c_{ij}(y_jx_i) = \Sigma_i\ \Sigma_j(c_{ij}y_j)x_i$

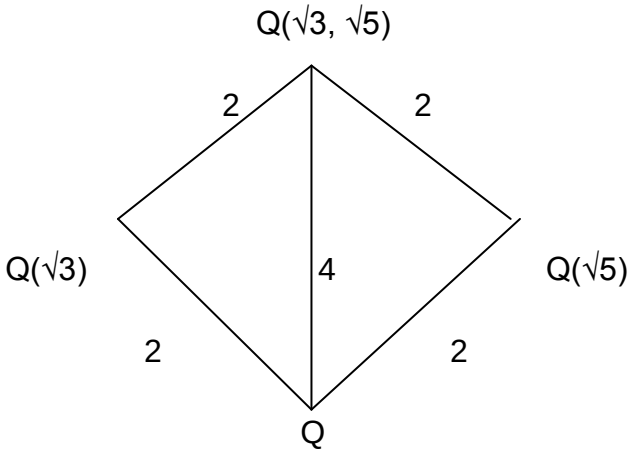
Then since each $c_{ij}y_j \epsilon E$ and X is a basis for k over E, we have

$\Sigma_j c_{ij}y_j = 0$ for each i

But each $c_{ij} \in F$ and Y is a basis for E over F, so each $c_{ij} = 0$.

This proves that the set YX is linearly independent over F.

Example: since {1, √3} is a basis for Q(√3 ,√5) over Q(√5) and {1,√5} is a basis for Q(√5) over Q, then as above theorem shows that {1, √3,√5,√15} is a basis for Q(√3, √5) over Q.



Consider Q ($\sqrt[3]{2}, \sqrt[4]{3}$).

Then [Q ($\sqrt[3]{2}, \sqrt[4]{3}$):Q].=12

For clearly,

[Q ($\sqrt[3]{2}, \sqrt[4]{3}$):Q] = [Q ($\sqrt[3]{2}, \sqrt[4]{3}$):Q($\sqrt[3]{2}$) [Q($\sqrt[3]{2}$):Q]

And

[Q ($\sqrt[3]{2}, \sqrt[4]{3}$):Q] = [Q ($\sqrt[3]{2}, \sqrt[4]{3}$):Q($\sqrt[4]{2}$) [Q($\sqrt[4]{2}$):Q]

Now:{1, $2^{1/3}$, $2^{2/3}$} is a basis for Q($\sqrt[3]{2}$) over Q

[Q($\sqrt[3]{2}$):Q]=3 and [Q($\sqrt[3]{2}, \sqrt[4]{3}$) : Q($\sqrt[3]{2}$)]=4, as

{1, $3^{1/4}$,$3^{2/4}$,$3^{3/4}$} is a basis for Q($\sqrt[3]{2}, \sqrt[4]{3}$) over Q($\sqrt[3]{2}$)

So,

[Q ($\sqrt[3]{2}, \sqrt[4]{3}$):Q] =12

(*) **To Show**: Q(√2, $\sqrt[3]{5}$) = Q (√2+ $\sqrt[3]{5}$)

Solution:

Claim 1: Q (√2+ $\sqrt[3]{5}$) ⊆ Q (√2, $\sqrt[3]{5}$)

Since √2, $\sqrt[3]{5}$ ∈Q(√2, $\sqrt[3]{5}$)

=> √2+$\sqrt[3]{5}$ ∈ Q(√2, $\sqrt[3]{5}$)

=> Q (√2+ $\sqrt[3]{5}$) ⊆ Q (√2, $\sqrt[3]{5}$)

Claim 2: Q(√2, $\sqrt[3]{5}$) ⊆ $Q(\sqrt{2}+\sqrt[3]{5})$

It is sufficient to prove: $\sqrt{2}$- $\sqrt[5]{5} \epsilon Q(\sqrt{2}+\sqrt[5]{5})$

$\sqrt{2} \in Q(\sqrt{2}+\sqrt[5]{5}) = Q(\alpha)$

Let $\sqrt{2}+\sqrt[5]{5} = \alpha(say)$

=> $\sqrt[5]{5}$= $\alpha-\sqrt{2}$(cubic both sides)

=> $5=\alpha^3-2\sqrt{2}-3\sqrt{2}\alpha^2+6\alpha$

=>$\sqrt{2}= (\alpha^3+6\alpha-5)/(2+3\alpha^2) \in Q(\alpha)$

=> $\sqrt{2}=(\alpha^3+6\alpha-5)(2+3\alpha^2)^{-1} \in Q(\alpha)$

Similarly, $\sqrt[5]{5} \epsilon Q(\alpha)$ so,

$\sqrt{2} - \sqrt[5]{5} \in Q(\alpha)$

PROPERTIES OF ALGEBRAIC EXTENSIONS

Theorem:

Algebraic over algebraic is algebraic

If K is an algebraic extension of E and E is an algebraic extension of F, then K is an algebraic extension of F.

Proof:

Let $a \in$ K, as K is algebraic over F so there is $b_0, b_1, \ldots, b_n \in$ E such that

$b_0+b_1a+\ldots+b_na^n=0$

Now

E is algebraic over F and $b_0, b_1, \ldots, b_n \in E$ so

$b_0, b_1, \ldots, b_n$ algebraic over F. So E |F is finite and E is isomorphic to

$F(b_0, b_1, \ldots, b_n)$

Therefore $F(b_0, b_1, \ldots, b_n)$ F is finite

=> $[F(b_0):F]$= finite

$[F(b_1):F]$ = finite

- - - - - - - - - -
- - - - - - - - - -
- - - - - - - - -- -

b_1 is algebraic over F

=> b_1 is algebraic over $F(b_0)$

Now, $[F(b_0b_1): F(b_0)]$=finite

$[F(b_0b_1): F]=[[F(b_0b_1): F(b_0)][F(b_0):F]$

(finite) (finite)

By separation we can write

$[F(b_0, b_1, \ldots, b_n):F]$= finite

[M:F]= finite

a satisfies

=> $b_0+b_1a+b_2a^2+ \ldots + b_na^n = 0$

=> a is algebraic over M

=> [M(a): M]= finite

Now,

[M(a): F] = [M(a):M][M:F]

= finite

=> M(a) is algebraic over F

=> ‘a’ is algebraic over F

=> k is algebraic over F.

Corollary:- Subfield of algebraic Elements

Let E be a field extension of field f.

Let S = {all elements of E which are algebraic over F}

Then ‘S’ is a sub field of E containing F.

Proof:

Let $a_1 b (b \neq 0) \in E$ are algebraic over F.

To show: a+b, a-b, ab, a/b are algebraic over F.

It is sufficient to show.

[F(a,b):F]= finite, as a+b, a-b, ab a/b ∈F(a,b)

Now;

[F(a,b):F] = [F(a,b): F(b)][F(b):F]

Also a is algebraic over F, it is clearly algebraic over F(b) .

Thus, both [F(a,b): F(b)] and [F(b):F] are finite.

(*) For any extension E of a field F, the subfield of E of the elements that are algebraic over F is called the algebraic closure of F in E. e.g. algebraic closure of Q in ℂ.

CHAPTER- 3

An Introduction to Galois Theory.

[1]Galois Theory

In the previous discussion we proved the existence of a finite extension of a field F which contains all the roots of a given polynomial f(x) whose coefficients are in F .The main idea of Galois theory (named for Evariste Galois , 1811 - 1832) is to consider the relation of the group of permutations of the roots of f(x) to the algebraic structure of its splitting field.

Basic Definitions

Automorphism, Group Fixing F, Fixed Field of H

A ring isomorphism φ of field E with itself is called an automorphism of E. The collection of automorphism of E is denoted by Aut (E)

➔ An automorphism $\varphi \in Aut(E)$ is said to fix an elements $\alpha \in E$ if $\varphi\alpha=\alpha$

If F is subset of E, then automorphism φ is said to fix F if $\varphi a=a \ \forall a \in F$

Any field has at least one automorphism, the identity map (trivial automorphism).

Definition: Let E be an extension field of the field F.

Let Aut(E/F) be the group of automorphisms of E which fix F

= set of F automorphism of E

= Galois group of E/F

= Gal (E/F)

i ,e. $Gal(E/F) = \{ \varphi | \varphi: E \to E \ \text{S.T.} \ \varphi(\alpha)=\alpha \ \forall \alpha \in F\}$

If H is a subgroup of Gal (E/F), the set

$E_H = \{x \in E \mid \varphi(x) = x \text{ for all } \varphi \in H\}$ is called fixed field of H

Example

1. Consider the extension $Q(\sqrt{2})$ of Q

Since $Q(\sqrt{2}) = \{ a+ b \sqrt{2} | a, b \in Q\}$

$\varphi: Q(\sqrt{2}) \rightarrow Q(\sqrt{2})$ such that $\varphi(a)=a \ \forall a \in Q$

$\varphi (a+ b \sqrt{2}) = \varphi (a)+ \varphi(b \sqrt{2})$

$= a+ \varphi (b) \varphi (\sqrt{2})$

$= a+ b \varphi (\sqrt{2})$

An automorphism φ of $Q(\sqrt{2})$ is determine if $\varphi(\sqrt{2})$ is to be calculate

$2= \varphi(2)= \varphi(\sqrt{2}\sqrt{2})= \varphi(\sqrt{2})\varphi(\sqrt{2})= (\varphi(\sqrt{2}))^2$

$\Rightarrow \varphi(\sqrt{2})= \pm\sqrt{2}$

this proves that the group $Gal(Q(\sqrt{2})|Q)$ has two elements, the identity mapping and mapping that sends $a+ b\sqrt{2}$ to $a- b\sqrt{2}$ the fixed field of $Gal(Q(\sqrt{2})|Q)$is just Q as everything is fixed by identity automorphism

i.e. $a+ b \sqrt{2} \rightarrow a+ b \sqrt{2}$

$a+ b \sqrt{2} \rightarrow a- b \sqrt{2}$

Which is equivalent to

$a +b \sqrt{2}= a-b \sqrt{2}$

$\Rightarrow b=0$

2. Consider the extension $Q(\sqrt[3]{2})$ of Q similarly as above example, an automorphism φ of $Q(\sqrt[3]{2})$ is completely determines by $\varphi(\sqrt[3]{2})$.

$\varphi(\sqrt[3]{2})$ is a cube root of 2.

Therefore $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}, \sqrt[3]{2}\omega$, or $\sqrt[3]{2}\omega^2$ where $\omega^3=1, \omega \neq 1$

Because φ ($\sqrt[3]{2}$) is real (subset of real number), the only possibility is Q ($\sqrt[3]{2}$) = $\sqrt[3]{2}$,

Hence

$a+b\sqrt[3]{2}$ -> $a+b\sqrt[3]{2}$

Gal (Q ($\sqrt[3]{2}$) |Q) has one elements and fixed field of Gal (Q ($\sqrt[3]{2}$) |Q) is Q ($\sqrt[3]{2}$)

3. Consider the extension Q (√3, √5) of Q.

As we known that Q (√3, √5) = {a + b √3 + c √5 + d √3 √5|a, b, c, d ∈ Q}

Any automorphism φ of Q (√3, √5) is completely determined by the two values φ (√3) and φ (√5). This time there are four automorphism:

ϵ	α	β	αβ
√3 -> √3	√3 -> -√3	√3 -> √3	√3 -> -√3
√5 -> √5	√5 -> √5	√5 ->- √5	√5 ->- √5

Gal (Q (√3, √5) |Q) = {ϵ, α, β, αβ} isomorphic to $Z_2 \oplus Z_2$

Let H= {Id, α}: α: a + b √3 -> a - b √3

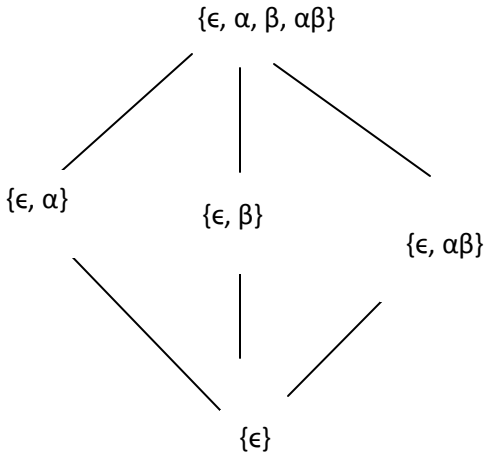
a + b √5 -> a + b √5

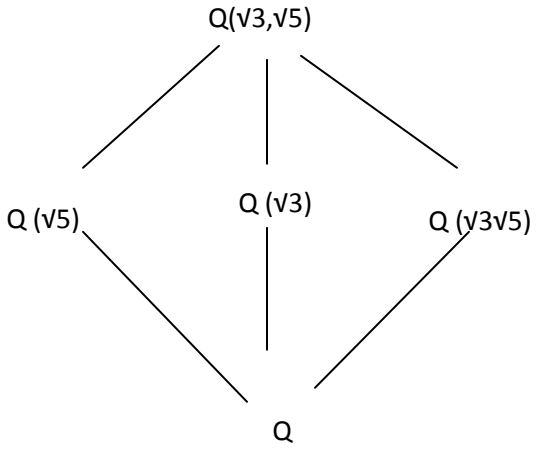
Fixed field of {ϵ, α} is Q (√5)

Fixed field of {ϵ, β} is Q (√3)

Fixed field of {ϵ, α β} is Q (√3√5)

The lattice of subgroup of Gal (Q (√3, √5) |Q) and the lattice of subfield of Q (√3, √5) are shown below:





[1]Hence we see that there is an intimate connection between the lattice of subfield between E and F and the lattice of subgroup of Gal (E/F).

Let A -> be the lattice of subfield of E containing F

B -> be the lattice of subgroup of Gal (E/F).

Then for each K in A , the group Gal (E/K) is in B and for each H in B, the field E_H is in A.

Define a mapping

g: A -> B by

g (K)=Gal(E/K)and

f: B -> A by

f (H)=E_H

If K and L belongs to A and K ⊆L then g(K) ⊇ g(L) similarly if G and H belongs to B and G⊆H then f(G) ⊇ f(H). Thus f and g are inclusion reversing mapping between A and B.

However, when E is suitably chosen extension of F, the fundamental theorem of Galois Theory says that f and g are inverse of each other so that the inclusions are equalities. In particular, f and g ate inclusion reversing isomorphism between the lattices A and B

[4]Galois Extension:

A finite extension E/F is said to be Galois extension if

$|Gal\ (E/F)| = [E: F]$

Example: In above example --- (1)

Gal (Q ($\sqrt{2}$) |Q) is Galois extension, whereas Gal (Q ($\sqrt[3]{2}$) |Q) in example --- (2) is not Galois extension.

Normal Extension:

let E be a finite extension of field F. The E is said to be normal extension of F if the fixed field of G (E/F) is F itself.

. Moreover –

These statements are equivalent

(i) E is normal extension of F
(ii) F is the fixed field of Gal(E/F)
(iii) [E:F]= |Gal (E/F)|

Results

(i) Let E be a normal Extension of F and H be a subgroup of Gal (E/F); let

$E_H = \{a \in E: \sigma(a) = a\ \forall\ \sigma \in H\}$ be the fixed field of H. Then

a. $[E:E_H]=|H|$
b. $H=Gal(E:E_H)$

(ii) E is a normal extension of F $\Leftrightarrow$ E is the splitting field of some polynomial over F

Conjugate element:

let E be a finite extension of a field F, then two elements α and β of a field E are said to be conjugate over F if they have the same minimal polynomial over F.

[1]FUNDAMENTAL THEOREM OF GALOIS THEORY

Statement:

Let F be a field of characteristic 0 or a finite field .If E is the splitting field over F for some polynomial in F[x], then the mapping from the set of subfields of E containing F to the set of subgroup of Gal(E/F) given by K→ Gal(E/K) is a one- to -one correspondence. Furthermore for any subfield K of E containing F.

1. [E: K] = |Gal (E/K)| and [K: F] =| Gal (E/F)|/ |Gal (E/K)|.

[The index of Gal (E/K) in Gal (E/F) equals the degree of K over F]

2. If K is the splitting field of some polynomial in F[x], then Gal (E/K) is normal subgroup of Gal (E/F) and Gal (K/F) is isomorphic to Gal (E/F)/ Gal (E/K).

3. K= Gal (E/K). [The fixed field of Gal (E/K) is K]

4. If H is a subgroup of Gal (E/F) ,then H= Gal(E/E_H)[The automorphism group of E fixing E_H is H]

Proof:

First we prove that there exists a one-one correspondence between the set of subfields of E containing F to the set of subgroup of Gal (E/F) given by

K→ Gal (E/K).

Let K be any subfield of E containing F and Gal (E/K) be group of all

K-automorphism of E.

Since F⊂K⊂E, so that Gal (E/K) ⊆ Gal (E/F). Also Gal (E/K) and Gal (E/F) are the subgroups of the group of all automorphism of E; therefore Gal (E/K) is a subgroup of Gal (E/F).

Thus for each subfield K of E containing, we can find a subgroup Gal (E/K) of Gal (E/F).

Consider a mapping ψ of the set of all subfields of E containing F into the set of all subgroups of Gal (E/F), defined by

Ψ (K) = Gal (E/K) for all subfield K of E containing F.

To prove ψ is one-one

Let k_1 and k_2 be any two subfields of E containing F and suppose that

Ψ (k_1) = Ψ (k_2)

⟹ Gal (E/k_1) = Gal (E/k_2)

∴ The fixed field of Gal (E/k_1) = the fixed field of Gal (E/k_2)

⇒ k_1 = k_2 (∵ E is a splitting over F

⇒ E is a normal extension of F)

Now to prove ψ is onto:

Let H be an arbitrary subgroup of Gal (E/F), then the fixed field of H denoted by E_H is

E_H = {aϵE : **Φ** (a)=a ∀ **Φ** ∈ H}

Then,

H= Gal (E/E_H).

This shows that each subgroup of Gal (E/F) is of the form Gal (E/E_H) such that

F⊆ E_H⊆E [E_H is fixed field] and corresponding to this subgroup Gal (E/E_H) there exist a subfield $E_H$of E containing F such that ψ (E_H)= Gal (E/E_H).

i) E is a normal extension of F and K is a subfield of E containing F such that

F⊆K⊆E then E is normal extension of K therefore we have

[E: F]= | Gal (E/F)| and

[E: K]= | Gal (E/K)|.

Moreover

[E: F]= [E: K] [K: F]

⟹| Gal (E/F)|= | Gal (E/K)| [K: F].

⟹ [K: F] = | Gal (E/F)|/ | Gal (E/K)|.

2. K is the splitting field of some polynomial in F[x], means K is the normal extension of F, to show Gal (E/K) is a normal subgroup of Gal (E/F).

For any $\sigma \in$ Gal (E/F) and $\psi \in$ Gal (E/K).

To show: $\sigma^{-1}\psi\,\sigma \in$ Gal (E/K)

Let α be any arbitrary element of K .Since K is a normal extension of F, so that the splitting field of the minimal polynomial of α over F is contained in K and every conjugate of α is therefore in K.

Since $\sigma(\alpha)$ is conjugate of α for any $\sigma \in$ Gal (E/F),

then $\sigma(\alpha) \in$ K . Thus for any automorphism $\psi \in$ Gal (E/K), $\psi(\sigma(\alpha)) = \sigma(\alpha)$

Now

$(\sigma^{-1}\psi\,\sigma)(\alpha) = \sigma^{-1}[\psi(\sigma(\alpha))]$

$= \sigma^{-1}(\sigma(\alpha))$

$= \alpha$

$\Longrightarrow \sigma^{-1}\psi\,\sigma \in$ Gal (E/K) $\quad \forall\ \sigma \in$ Gal (E/F)

$\Psi \in$ Gal (E/K).

Let K is the normal extension of F. Let σ be any element of G (E|F).Define a mapping $\sigma'$of K into E be splitting $\sigma'(\alpha) = \sigma(\alpha)\ \forall\ \alpha \in$ K. Since σ is an F- automorphism of E and K is a normal extension of F, so that K = F (α), therefore σ' is F –automorphism of K

i.e., $\sigma' \in G(K|F)$

Thus $\sigma(K) = \sigma'(K) = K$.

Now consider a mapping

$\mathbf{\Phi}: G(E|F) \rightarrow G(K|F)$ by setting

$\mathbf{\Phi}(\alpha) = \sigma' \ \forall \ \sigma \in G(E|F)$

This mapping $\mathbf{\Phi}$ is a group homomorphism; for if σ_1 and σ_2 are any two elements of G(E|F) and $\alpha \in K$, then

$(\mathbf{\Phi}(\sigma_1\sigma_2))(\alpha) = ((\sigma_1\sigma_2)')(\alpha)$ [By above define]

$= (\sigma_1\sigma_2)(\alpha)$

$= \sigma_1(\sigma_2(\alpha))$

and $(\mathbf{\Phi}(\sigma_1)\mathbf{\Phi}(\sigma_2))(\alpha) = \mathbf{\Phi}(\sigma_1)(\mathbf{\Phi}(\sigma_2)(\alpha))$

$= (\mathbf{\Phi}(\sigma_1))(\sigma'_2(\alpha))$

$= (\mathbf{\Phi}(\sigma_1))(\sigma_2(\alpha))$

$= \sigma_1'(\sigma_2(\alpha))$

$= \sigma_1(\sigma_2(\alpha))$

So, $\mathbf{\Phi}(\sigma_1\sigma_2) = \mathbf{\Phi}(\sigma_1)(\sigma_2)$

Consider any ψ ∈ Gal (K/F), then

Ψ (α) is conjugate of α over F, so there exists an F-automorphism σ of E

Such that σ (α) = Ψ (α) .

Also σ and Ψ are both identity of F and K and K =F(α),

So that σ (a) = Ψ (a) $\forall$ a ∈ F (α) = K.

$\therefore$ ψ = σ'= $\boldsymbol{\Phi}$ (α)

Hence f is onto

Furthermore,

Kernel $\boldsymbol{\Phi}$ = $\{\sigma \in$ G (E|F) :(σ) =$\boldsymbol{I}$, the identity of Gal (K/F)$\}$

$= \{ \sigma \in$ G (E|F):$\sigma' = \boldsymbol{I}\}$

$= \{\sigma \in$ G (E|F):σ' (α) =$\boldsymbol{I}$ (α) $= \alpha \ \forall \alpha \epsilon K\}$

$= \{\sigma \in$ G (E|F) : σ (α) =$\alpha \ \forall \alpha \epsilon K\}$

= Gal (E/K)

Then by Fundamental theorem of homomorphism of groups

Gal (K/F) is isomorphic to Gal (E/F)/ Gal (E/K).

3. E is a normal extension of K (from above discussion)

So, by definition of normal extension the fixed field of G (E|K) is K.

4∵H is a subgroup of Gal (E/F) so that H ⊂ Gal (E/F)

Also is the fixed field of H, then we have

E_H = {a ∈ E | σ (a) =a∀ σ ∈H}

∵E_H is subfield of E.

Since E is a normal extension of F, so that E is a finite extension of F

Gal (E/E_H) |≤ [E: E_H] ……(i)

Now Gal (E/E_H) = {σ∈A (K); (a) =a ∀a∈E_H} ……(ii)

Let σ be any automorphism in H, then

σ∈H⟹ σ (b) =b∀ b∈E_H [using ii]

⟹σ∈ Gal (E/E_H) [using ii]

Therefore H ⊂ Gal (E/E_H)

Therefore |H|≤| Gal (E/E_H)| …… (iii)

From (i) and (iii)

|H|≤| Gal (E/E_H) |≤ [E: E_H]

and |H|≤| Gal (E/E_H) |≤ |H|

⟹|H|=| Gal (E/E_H)|

Also H is a subgroup of Gal (E/E_H)

Hence H=Gal (E/E_H).

Summary

In the first chapter of project –I have discussed some fundamental concepts which are related and useful in the Field Theory and Galois Theory like –Euclidean domains, Principle ideal domain and Unique Factorization Domain (which has an important role basically in the fundamental theorem of Field Theory) and relation among them.

In the main discussion, i.e. from the 2^{nd} chapter it is starting from definition, different examples, and related theorem of Extentions Field, Splitting Fields, Existence of Splitting Fields, Algebraic Extentions, Characteristics of Extentions, Degree of extension and the properties of Algebraic Extentions.

In the last chapter (Galois Theory) – I discussed mainly Fundamental Theorem of Galois Theory that's show the intimate connection between the lattices of Subfield between E (Extentions Field) and F (Field) and the lattice of subgroups of Gal (E/F).

References

[1] Joseph A. Gallian, Contemporary Abstract Algebra, New Delhi Narosa Publishing House , 1999.

[2] David S. Dummit & Richard M.Foote , Abstract Algebra ,John Wiley & Sons,Inc. New York.

[3] P.B.Bhattacharya, S.K. Jain,S.R.Nagpal- Basic Abstract Algebra Cambridge University Press ,1995.

[4] John B. Fraleigh, A First Course In Abstract Algebra, Pearson Education (Singapur) Pte.Ltd. , Indian Branch, 482 F.I.E. Patparganj,New Delhi.

[5] Bhupendra Singh, Advance Abstract Algebra Pragati Prakashan, Meerut 1999